一种改进的 CCN 兴趣包泛洪攻击防御方法 *

吴　浔，凌　捷

(广东工业大学 计算机学院，广州 510006)

摘　要：内容中心网络（content-centric networking，CCN）中兴趣包泛洪攻击（interest flooding attack，IFA）是 CCN 网络安全的研究热点问题。为了提高 CCN 防御 IFA 的能力，针对不同防御方法进行了研究，提出一种改进的 CCN 兴趣包泛洪攻击防御方法。该方法根据 CCN 流平衡原理，采用恶意前缀溯源的方式，实现对 IFA 的快速检测，并通过改进和式增加积式减少(additive increase multi-plicative decrease，AIMD)算法，实现对 IFA 的防御。安全性分析表明，该方法在面对 IFA 时，能够更快的作出反应；并且相比于其他 IFA 防御方法，该方法在保证安全性的前提下，降低了 CCN 路由器在检测 IFA 时的计算开销。

关键词：兴趣包泛洪攻击；恶意前缀溯源；内容中心网络；CCN；IFA

中图分类号：TP393.08　　doi: 10.19734/j.issn.1001-3695.2018.09.0754

Improved defense method for interest flooding attack in CCN

Wu Xun, Ling Jie

(*School of Computer*, *Guangdong University of Technology*, *Guangzhou* 510006, *China*)

Abstract: The interest flooding attack (IFA) in content-centric networking (CCN) is a hot topic of research on CCN network security. In order to improve the ability of CCN to defend against IFA, this paper studied different defense methods and proposed an improved defense method for interest flooding attack in CCN. According to the CCN flow balance principle, the method used the method of malicious prefix tracing to achieve fast detection of IFA, and the defense against IFA was achieved by improving the Additive Increase Multi-plicative Decrease (AIMD) algorithm. The security analysis shows that the proposed method can defend faster when it in the face of IFA. Compared with other defense methods, this method reduces the computational cost of the CCN router when detecting IFA under the premise of ensuring security.

Key words: intersting flooding attack; malicious prefix traceability; content-centric networking; CCN; IFA

0　引言

内容中心网络（CCN）自提出以来受到广泛的关注，已成为未来互联网架构体系中极具前景的架构之一[1]。CCN 命名数据，通过兴趣包（interest packet）请求相应数据，服务器或路由器返回相应的数据包（data packet）。每个 CCN 路由器至少含有三个数据结构：内容缓存（content store，CS）、待定请求表（pending interest table，PIT）、向前转发表（forwarding information base，FIB）[2]。其中，CS 负责缓存收到的数据包，PIT 负责记录请求的兴趣包以及其到来的接口，方便数据包的响应，FIB 负责进行路由转发。

CCN 路由器的结构能够解决传统 IP 网络中源地址伪造、针对特定主机泛洪攻击等威胁。但是新的结构也带来了新的安全隐患，其中对 CCN 威胁最大的隐患就是兴趣包泛洪攻击。由于路由器需要将收到但未被 CS 满足的兴趣包的内容名称信息记录在 PIT 表中，攻击者可以利用该特性，伪造大量不会被 CS 满足的恶意兴趣包进行兴趣包泛洪攻击，通过耗尽路由器的 PIT 空间，使正常用户的请求被路由器抛弃，从而达到拒绝服务攻击的目的。

1　IFA 防御方法研究现状

在此背景下，国内外很多研究机构都在为解决 CCN 中的兴趣包泛洪攻击进行大量的科学实验与研究。唐建强，周华春等人提出协同防御方法[3]，使用 AIMD 算法限制带有异常内容名称前缀的兴趣包的转发速率。Alexander 教授及其团队成员提出了基于端口流量限制的 IFA 攻击防御方法[4]，该算法主要是使每个出端口都有相应的限制值，当每个端口发出的兴趣包超出了该限值，这些报文将在队列中挂起。当允许发出报文的时候，从入端口的队列中均等地将接受的报文转发出去。Cheng 等人[5]提出一种基于满足率的反馈防御方法。该方法根据通过检测兴趣包的满足率，判断是否发生 IFA，然后通过接口限制对 IFA 进行防御。Gasti 等人[6]提出根据 CCN 流平衡原理，判断 IFA 攻击是否发生，进而对其进行防御。Dai 等人[7]提出一种兴趣包溯源 (interest trace back)机制，通过 CCN 节点构造一条抑制信息，逐跳向攻击源头传递抑制信息。收到抑制信息的路由器再判定出恶意前缀后，通过伪造数据包并回复恶意兴趣包请求，使路由器 PIT 中的非法条目因收到“对应数据包”而被满足，并最终反向定位到接入路由器，从而在接入路由器入口处限制 IFA 恶意兴趣包的准入速率。Compagno 等人[8]提出 Poseidon，根据路由器中每个接口接收兴趣包与发出数据包的比例和 PIT 的使用率来判断不同接口是否发生兴趣包泛洪攻击。Cheng 等人[9]提出网络的自相似性特性可以很好地描述流量特性，可以用网络的自相似性作为流量异常检测的基础，根据流量异

收稿日期：2018-09-17；**修回日期：**2018-11-12　**基金项目：**广东省科技计划资助项目（2017B090906003）；广州市重大科技专项资助项目（201604010063，201802010043，201807010058）

作者简介：吴浔（1994），男，江西九江人，硕士研究生，主要研究方向为内容中心网络兴趣包泛洪攻击防御方法（1129852280@qq.com）；凌捷（1964），男，广东梅州人，教授，硕导，博士，主要研究方向为网络信息安全与智能视频处理技术.

常信息判断是否发生 IFA。Garcia-Luna-Aceves 等人[10]提出使用 CCN-GRAM (gathering of routes for anonymous messengers)策略替代现有的 CCN 路由策略，以期从根源上杜绝 IFA 攻击。通过强制中间路由器对兴趣包签名验证可以一定程度上抑制 IFA 攻击。然而，强制计算有可能导致隐私问题[11]，并且可能会产生一种通过强制计算攻击路由器的威胁。针对这个问题，Ribeiro 等人[12,13]提出了一种 CCNCheck 机制，该机制要求路由器以动态的概率进行签名验证。另外，由于软件定义网络(software defined network，SDN)的网络控制器拥有全网视图，可以快速准确的搜集全网监控节点的兴趣包信息，因此能够及时发现网络异常攻击流量，避免重复检测和过分响应，快速抑制攻击源并保护合法用户[14,15]。

在以上的各种防御方法中，大多数都涉及到 IFA 的检测技术，首先需要检测到发生了 IFA 攻击，以及检测出哪些内容名称前缀是恶意的，然后根据这些恶意的前缀信息进行防御。本文提出一种新的 IFA 检测方法，该方法充分发挥网络设备的自身特性，能很快的找到网络中具有恶意前缀的兴趣包，并将该恶意前缀信息通过溯源的方式告诉网络中的其他路由器，当网络中其他设备收到该错误信息时，通过改进的 AIMD 算法[3]对那些带有恶意内容名称前缀的兴趣包进行防御。本文方法相对于文献[3]，不再需要检测 PIT 信息并进行繁杂的计算就可以判断出是否发生了兴趣包泛洪攻击，本文方法只需检测其他路由器回传的数据包的标记位即可。另外，本文方法改进了文献[3]的 AIMD 算法，使得该算法适应于本文的防御方法，且可以通过最短前缀匹配的方法，把恶意前缀收束到一个比较小的空间中，不会给路由器存储设备带来压力。

2　恶意前缀溯源防御 IFA 攻击

2.1　恶意前缀溯源

CCN 中路由器转发兴趣包时，根据最长前缀匹配的原则查询 FIB 得到对应的接口，然后根据转发策略从其中的部分或全部接口发送兴趣包，若在 FIB 中匹配不到某个兴趣包的内容名称，则认为该兴趣包是错误兴趣包，并将其丢弃。此外，当兴趣包一直转发到了对应的内容服务器，但是服务器中没有该兴趣包所请求的数据时，也做同样的处理。

根据 CCN 流平衡原理，CCN 网络传输机制维持兴趣包和数据包的一种内在平衡。即每向上游发送一个兴趣包，最多只会产生一个数据包向下游回复。实际上破坏这种平衡的原因就是，在路由转发策略中，遇到内容名称出错的兴趣包时直接将其丢弃。无论这些名称出错的兴趣包是否是恶意兴趣包，实际上在整个网络中总是存在唯一知道这些名称出错兴趣包的设备，就是丢弃内容名称出错兴趣包的设备，可能是 CCN 路由器或者内容服务器。根据 CCN 网络的这种特性，本文提出一种改进的 CCN 兴趣包泛洪攻击防御方法。

在 CCN 路由器中，维护有三个空间：CS、FIB、PIT。路由器收到兴趣包后，若 CS 空间和 PIT 中都没有相关信息，则查找 FIB，存在该内容名称前缀的域时，转发该兴趣包到下一跳，并在 PIT 中添加新条目。若 FIB 表中未检索到该前缀域，则回复一个带有标记位的数据包并丢弃该兴趣包。该数据包的内容为内容名称、标记位以及最短异常内容名称，路由器收到数据包时检查标记位，若是被丢弃的兴趣包则表明对应内容名称的兴趣包为异常兴趣包，首先删除 PIT 表中条目，然后采用 AIMD 算法限制带有异常内容名称兴趣包的传输速率。若兴趣包能够一直到达服务器，但服务器中不存在所请求的文件，即兴趣包所请求的内容在服务器中是不存在的。则服务器同样以这种带标记的数据包的形式进行回复。具体处理流程如图 1、2 所示。

2.2　恶意前缀的防御

本文改进了文献[3]中的 AIMD 算法对收到的带有特殊标记的数据包进行处理。相对于文献[3]中的 AIMD 算法改进的地方有：增加一个空间 Queue[b,Rb,t]，用于记录异常内容名称的最短前缀，该前缀的转发速率，以及存在的时间；使用最短异常前缀匹配的原则收束异常的名称前缀；增加了对溯源数据包进行标记，设置溯源数据包的内容，以及对标记进行检测等步骤，使其更加适应本文的恶意前缀溯源方法，如算法 1 所示。

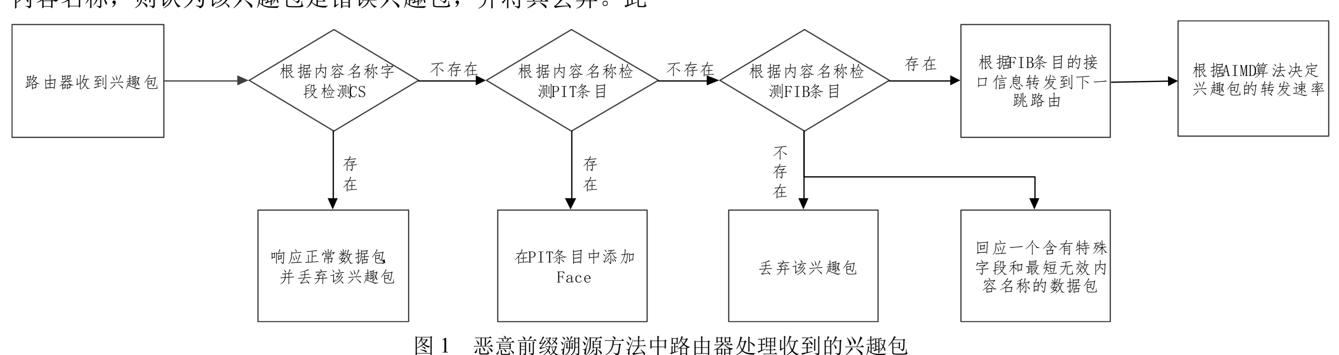


图 1　恶意前缀溯源方法中路由器处理收到的兴趣包

Fig. 1　Router processes the received interest packet in the malicious prefix traceability method.

路由器收到数据包
检测特殊字段
正常数据包
根据PIT条目的Face信息转发该数据包
根据缓存策略决定是否缓存到CS中，然后删除PIT条目
名称异常数据包
将数据包内容提取返回到AIMD算法
根据PIT条目的Face信息转发该数据包
不在CS中缓存该数据包，转发后直接删除

图 2　恶意前缀溯源方法中路由器处理收到的数据包

Fig. 2　Router processes the received data packet in the malicious prefix traceability method.

以下简单介绍最短异常前缀。例如，某内容名称为 N1/N2/N3/N4/…，FIB 中存在目标网域为 N1/N2/的条目，于是通过最长前缀匹配可以将带有该内容名称的兴趣包转发到条目 N1/N2/所记录的下一跳路由，但是若在下一跳的路由器 FIB 中不存在网域为 N1/N2/N3/的条目，于是路由器将抛弃该兴趣包，并根据恶意前缀溯源策略返回一个数据包，这个数据包的内容名称为相应兴趣包的内容名称 N1/N2/N3/N4/…，数据包的内容为下一跳不可达的最短前缀 N1/N2/N3/，这个最短前缀 N1/N2/N3/就是最短异常前缀。

使用 AIMD 算法，每当收到一个攻击兴趣包时，下一个具有相同内容名称前缀的攻击兴趣包的转发速率就衰减 e^(-C)，而且每当有新的带有标记的数据包到来，根据算法 1，比较数据包的内容和 Queue[]中的前缀信息，若 Queue[]的某条目包含了该最短恶意前缀时，算法将收束该条目的内容名称前缀为新的最短恶意前缀。所以算法中 Queue[]能够起到收束最短恶意前缀的作用。对于随机生成恶意兴趣前缀的攻击兴趣包而言，能够快速的衰减其转发速率，起到防御 IFA 的目的。

算法 1　基于 AIMD 的异常名称兴趣包速率限制方法

```
//  C 为大于 1 的常数，例如 C = 10，T 为默认时间。
struct{
string countName_short;          //最短异常前缀
unsigned double forward_v;       //转发速率
unsigned int time;               //距离上一次收到该数据的时间
int find_long(string) //寻找 Queue 中被字符串包含的最长前缀位置
int find_short(string)  //寻找 Queue 中包含字符串的最短前缀位置
insert();                      //插入一个新的条目
updata();
//自动降低各个条目的 time 值，如果有 time 值为 0 的条目则删除该条目。
}Queue[];
struct{
string countName;        //数据报内容名称信息
int flag
//数据报特殊位，判断是兴趣包还是数据包。若是 0 表示兴趣包，1 表示正常数据包，2 表示异常数据包。
string data;               //数据报的所包含的数据
name_short();              //返回最短无效内容名称
}Datagram;
switch(Datagram.flag)
case 0:                    //兴趣包
    if CS.find(Datapram.countName) || PIT.find(Datagram.countName) || FIB.find(Datapram.countName):
        forward(Datagram);      //默认方式转发兴趣包
        return 0;
    if Queue.find_long(Datagram.countName):
        int i = Queue.find_long(Datagram.countName);
//返回最长前缀匹配的下标
        forward(Datagram, Queue[i].forward_v);
//以速率 forward_v 转发兴趣包
        return 0;
//若 CS、PIT、FIB、Queue 中都未匹配到该内容名称兴趣包
int flag=2;
data = Datapram.name_short();
    datapack = make_datapack(Datapram.countName, flag, data);
//产生一个内容名称为兴趣包内容名称，特殊位为 2，内容为兴趣包的最短无效名称的数据包
    delete Datagram;
    return datapack;          //返回一个记录异常的数据包
end if
case 1:                       //正常数据包
//此处还需判断 Queue 中是否有对应前缀，有则删除，并将速度 y+C
    Queue.updata();
    return Datagram;        //真正返回数据包
end if
case 2:                      //异常数据包
Queue.updata();  //更新队列
if !Queue.find_long(Datagram.data) &&
! Queue.find_short(Datagram.data):
//若即找不到最短匹配，又找不到最长匹配，则增加新的条目
time = T;
forward_v = init_forward_v;
        countName_short = Datagram.data;
        Queue.insert(countName_short, forward_v, time);
//插入新的条目
else: if Queue.find_short(Datagram.data):
    //若在 Queue 中能找到最短匹配，更新条目
int i = Queue.find_short(Datagram.data);
Queue[i].forward_v *= e^(-C)
Queue[i].time = T;
Queue[i].countName_short = Datapram.data;
    else:    //若能找到最长前缀匹配，更新该条目
int i = Queue.find_long(Datagram.data);
        Queue[i].forward_v *= e^(-C);
Queue[i].time = T;
end if
```

2.3　举例

图 3 描述了一个简单的溯源防御例子，假设所有路由器的 CS 为空，路由器 CCN-R1 的 FIB 表中有 3 个条目：www/youku、www/baidu、www/bilibili；CCN-R2 的 FIB 表有一个条目：www/youku/com；CCN-R3 的 FIB 表条目：www/baidu/com；CCN-R4 的 FIB 表条目：www/bilibili/com。攻击者发送一个内容名称为 www/baidu/cn 的兴趣包到 CCN-R1，根据最长前缀匹配的原则，CCN-R1 将该兴趣包转发至 CCN-R3，此时由于兴趣包的内容名称为 www/baidu/cn 在 CCN-R3 的 FIB 表中找不到对应的条目，当前的处理方法是直接丢弃该兴趣包，本文的做法是在此时回复一个带标记的数据包。

当 CCN-R1 收到数据包时，检测数据包的标记位，若发现是恶意前缀溯源的数据包，则通过 AIMD 算法在队列 Queue[]中新增一个条目记录该前缀 www/baidu/cn，并在下一次收到具有该前缀的兴趣包时，限制其转发速率。

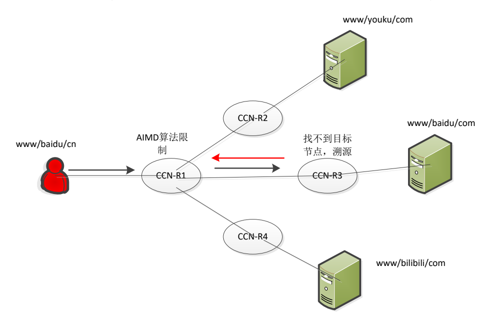


图 3　恶意前缀溯源防御 IFA 的一个例子

Fig. 3　Example of malicious prefix traceability defense IFA

图 4 描述了一个 Queue[]队列收束恶意内容名称的例子。图中 1、2、3、4 表示攻击者通过程序生成不同的恶意内容名称发送到网络，并在网络中传播，5、6、7 表示路由器或服务器返回的带有恶意内容名称的受标记的数据包传播路径，若发送的是内容名称为 a/b/c/[非 d]/[任意值]时，将其收束为同一个条目，并降低其转发如 c 路由 Queue[]所示，若在 Queue[]队列中有条目收到了正确的数据包，则删除该前缀并将速度 v 增加 C。

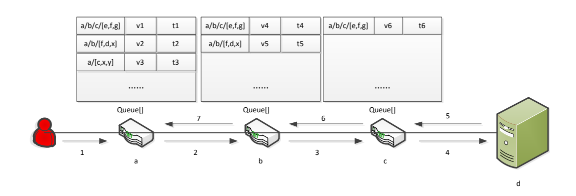


图 4 Queue 队列收束恶意内容名称的一个例子

Fig. 4 Example of a Queue queue that pack malicious content names

3 安全性分析

3.1 恶意前缀溯源分析

本文的恶意前缀溯源的思想早在文献[7]中已经被提出。文献[7]提出兴趣包回溯机制，在判定出恶意前缀后，路由器通过伪造数据包并回复恶意兴趣包请求，使路由器 PIT 中的非法条目因收到"对应数据包"而被满足，并最终反向定位到接入路由器，从而在接入路由器入口处限制 IFA 恶意兴趣包的准入速率。但是文献[7]中没有给出具体策略布置的位置，而且也需要首先检测到恶意兴趣包才能针对性的进行防御。本文相比于文献[7]，首先明确了布置策略的具体位置为全网路由器和内容生产者，其次本文不需要检测恶意兴趣包，可以直接对带有恶意内容名称的兴趣包进行溯源，再结合 AIMD 算法，可以起到很好的防御 IFA 攻击效果。

3.2 AIMD 算法安全性分析

本文改进了 AIMD 算法，相比于文献[3]中的 AIMD 算法，增加了一个 Queue[]空间。在文献[3]中实际上也运用到一个类似的空间，只是没有对其进行详细的描述。如 Fig.4 所示，本文对该空间进行详细的描述，其作用是记录最短恶意前缀，能够对攻击者所产生的大量不同的恶意前缀进行收束，图中，Queue[]条目数与网络的跳数有关，根据 TCP/IP 网络中 RIP 协议的跳数限制可知在真实网络中网络的跳数不会超出一定值，因此本文所要求的空间并不会给路由器带来太大的空间负担。

本文方法相比于文献[3]能够保证安全性。本文方法对 IFA 的防御策略主要依赖于 AIMD 算法，虽然本文对该算法进行改进，但是在关键的限制恶意前缀的转发速率上并没有太大改变，在文献[3]中，证明了这种限制带有恶意前缀兴趣包的转发速率的方法能够起到较好的防御作用。因此，本文改进的 IFA 防御方法能够保证安全性。

3.3 效率分析

本文方法在面对兴趣包泛洪攻击时，在反应速度方面，相比于文献[3]得到了一定程度的提高。在文献[3]中，需要检测 PIT 的使用率以及兴趣包的满足率，它需要等待 PIT 空间被填满或即将填满，以及等待一定数量的兴趣包未被满足，才能通过算法判断发生了 IFA 攻击。

在此过程中，主要依据两个参数：PIT 使用率 φ 和兴趣包满足率 S。用 $t_1, t_2, \cdots$, t_n 表示时刻，用 $I(t_n)$ 和 $D(t_n)$ 表示第 n 段时间段内到达路由器的兴趣包和数据包数量，则到达路由器的兴趣包的历史平均值和数据的历史平均值可以分别表示为：$\bar{I}(t_n)=(1-\alpha)\bar{I}(t_{n-1})+\alpha\bar{I}(t_n)$，$\bar{D}(t_n)=(1-\alpha)\bar{D}(t_{n-1})+\alpha\bar{D}(t_n)$ 其中 $0<\alpha<1$ 是惯性系数，表示长时间段内平均数据数量对当前数据数量的敏感程度。tn 时刻路由器的兴趣包满足率为：$S(t_n)=\bar{D}(t_n)/\bar{I}(t_n)$，由于 CCN 中一个兴趣包只能被一个数据包满足，因此正常情况下，兴趣包满足率应该为 100%。当 PIT 使用率大于阈值时，表明 PIT 的兴趣包数量超出预警值，当兴趣包满足率值低于阈值时，表明兴趣包数据包一一对应的关系出现异常，通过这两个值的变化来判断是否发生了 IFA 攻击。

而本文的方法可以做到在一个往返时间内就能对具有恶意前缀的兴趣包进行限速。并且也不需要如上所述的计算过程，只需要等待下一个节点返回恶意内容名称即可。由于 PIT 条目的过期时间远远大于网络中的平均往返时间，因此文献[3]在面对 IFA 时，不可能在一个往返时间内作出反应。因此在检测 IFA 是否发生方面，本文相比于文献[3]具有一定的进步。

表 1 将本文的方法与其他 IFA 防御方法进行对比，可以更加详细的看到各种方法的工作方式以及部署方式。

表 1 IFA 防御技术比较

Table 1 IFA defense technology comparison

	攻击检测		攻击防御			部署位置
	攻击检测方法	检测粒度	是否溯源	速率限制方法	速率限制粒度	
基于满足率的反馈方法[5]	兴趣包满足率	异常接口	单跳回溯	基于兴趣包满足率的速率限制	按接口限制	全网路由器
Poseidon[8]	PIT使用率和兴趣包满足率	异常接口	单跳回溯	动态阈值	按接口限制	全网路由器
Tracback[7]	PIT使用率	异常名称	逐跳回溯	边界路由器限制	按攻击者限制	特定位置
基于前缀识别的协同防御方法[3]	PIT使用率和兴趣包满足率	异常前缀	单跳回溯	基于AIMD的异常前缀速率限制	按前缀限制	全网路由器
SDN[14,15]	兴趣包满足率和PIT到期率	异常接口和异常前缀	单跳回溯	SDN流调控	按前缀限制	监控路由器中央控制器
本文方法	数据包的标记位	异常前缀	逐跳回溯	基于AIMD的异常前缀速率限制	按前缀限制	全网路由器和内容生产者

值得一提的是，本文方法通过溯源带有标记的数据包的方式，将恶意内容名称告知整个网络，而如表中所示多数 IFA 防御方法需要用到恶意内容名称信息。因此本文的方法也可以与其他 IFA 的防御技术进行有效的合作部署，这种合作可以使得其他的 IFA 防御技术不再依赖于 IFA 检测模块，可以提高这些防御技术在检测 IFA 时的效率。

例如，本方法与协同防御策略结合，可以通过增加协同防御包模块，使得其他路由器快速知道新的恶意前缀信息。而本文的方法中，必须是恶意兴趣包经过的路径上的路由才会对其进行防御。结合之后，可以有效提高整个网络对恶意兴趣包的防御能力。与 SDN 方式结合时，当溯源数据包到达监控路由器时，将恶意内容名称前缀发送给中央控制器，可以节省传统技术的检测恶意内容名称的时间等。

4 结束语

文献[3]的协同防御策略通过检测路由器中的 PIT 使用率和兴趣包的满足率，能够有效的检测出是否发生了兴趣包泛洪攻击，然后通过 AIMD 算法，对检测到的带有恶意前缀的兴趣包进行防御。该方法本身对 CCN 中的兴趣包泛洪攻击具有十分优秀的防御能力。但是，文献[3]的方法在检测 IFA 方面也存在不足之处，根据 CCN 流平衡原理，在网络中实际上有知道恶意前缀信息的设备，因此不需要通过检测路由器中的 PIT 使用率和兴趣包的满足率就能够得到恶意兴趣包的前缀信息。本文利用网络中这些知道恶意前缀信息的设备对恶意前缀进行溯源，可以在一个往返时间内对这些恶意前缀进行防御。相比于文献[3]的方法，在应对兴趣包泛洪攻击时，反应速度上得到了提高，另外在不改变 AIMD 算法的核心情况下，改进 AIMD 算法使其适用于新的检测技术，这样就保证的安全性。总而言之，本文方法相比于文献[3]，在保证了安全性的前提下，提高了对兴趣包泛洪攻击的反应速度且降低了 CCN 路由器检测 IFA 时的计算开销。

参考文献：

[1] 李杨，辛永辉，韩言妮，等. 内容中心网络中 DoS 攻击问题综述 [J]. 信息安全学报, 2017, 2 (1): 91-108. (Li Yang, Xin Yonghui, Han Yanni, *et al.* Overview of DoS attacks in content center networks [J]. Journal of Information Security, 2017, 2 (1): 91-108.)

[2] 陈震，曹军威，尹浩. 内容中心网络体系架构 [M]. 北京：清华大学出版社，2014. (Chen Zhen, Cao Junwei, Yin Hao. Content center network architecture [M]. BeiJing: Tsinghua University Press, 2014.)

[3] 唐建强，周华春，刘颖，等. 内容中心网络下基于前缀识别的兴趣包泛洪攻击防御方法 [J]. 电子与信息学报，2014, 36 (7): 1735-1742. (Tang Jianqiang, Zhou Huachun, Liu Yi, *et al.* Mitigating interest flooding attack based on prefix identification in content-centric networking [J]. Journal of Electronics & Information Technology, 2014, 36 (7): 1735-1742.)

[4] Afanasyev A, Mahadevan P, Moiseenko I, *et al.* Interest flooding attack and countermeasures in Named Data Networking [C]//Procof IFIP Networking Conference. Piscataway, NJ: IEEE Press, 2013: 1-9.

[5] Cheng Yi, Afanasyev A, Moiseenko I, *et al.* A case for stateful forwarding plane [J]. Computer Communications, 2013, 36 (7): 779-791.

[6] Gasti P, Tsudik G, Uzun E, *et al.* DoS and DDoS in Named Data Networking [C]//Proc of the 22nd International Conference on Computer Communications and Networks. Piscataway, NJ: IEEE Press, 2012: 1-7.

[7] Dai Huichen, Wang Yi, Fan Jindou, *et al.* Mitigate DDoS attacks in NDN by interest traceback [C]//Proc of Computer Communications Workshops.Piscataway,NJ: IEEE Press, 2014: 381-386.

[8] Compagno A, Conti M, Gasti P, *et al.* Poseidon: mitigating interest flooding DDoS attacks in named data networking [C]// Local Computer Networks. Piscataway, NJ: IEEE Press, 2013: 630-638.

[9] Cheng Xiaorong, Xie Kun, Wang Dong. Network traffic anomaly detection based on self-similarity using hht and wavelet transform [C]// Proc of International Conference on Information Assurance and Security. Piscataway, NJ: IEEE Press, 2009: 710-713.

[10] Garcia-Luna-Aceves J J, Barijough M M. Content-centric networking using anonymous datagrams [C]//Proc of IFIP Networking Conference. Piscataway, NJ: IEEE Press, 2016: 171-179.

[11] Lauinger T. Security & scalability of content-centric networking [D]. Darmstadt: Technische Universität Darmstadt, 2010.

[12] Ribeiro I, Rocha A, Albuquerque C, *et al.* On the possibility of mitigating content pollution in Content-Centric Networking [C]// Local Computer Networks. Piscataway, NJ: IEEE Press, 2014: 498-501.

[13] Ribeiro I, Rocha A, Albuquerque C, *et al.* Content pollution mitigation for Content-Centric Networking [C]// Network of the Future. Piscataway, NJ: IEEE Press, 2017: 1-5.

[14] Salah H, Wulfheide J, Strufe T. Coordination supports security: a new defence mechanism against interest flooding in NDN [C]// Local Computer Networks. Piscataway, NJ: IEEE Press, 2016: 73-81.

[15] Salah H, Wulfheide J, Strufe T. Lightweight coordinated defence against interest flooding attacks in NDN [C]//Proc of IEEE Conference on Computer Communications Workshops. Piscataway, NJ: IEEE Press, 2015: 103-104.